

JOeSandbox Cloud BASIC



ID: 756033

Sample Name: payment
copy.exe

Cookbook: default.jbs

Time: 14:54:07

Date: 29/11/2022

Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents	2
Windows Analysis Report payment copy.exe	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Process Tree	4
Malware Configuration	4
Threatname: Agenttesla	4
Yara Signatures	4
Memory Dumps	4
Unpacked PEs	5
Sigma Signatures	5
Snort Signatures	5
Joe Sandbox Signatures	5
AV Detection	5
System Summary	5
Hooking and other Techniques for Hiding and Protection	6
Malware Analysis System Evasion	6
Stealing of Sensitive Information	6
Remote Access Functionality	6
Mitre Att&ck Matrix	6
Behavior Graph	7
Screenshots	7
Thumbnails	7
Antivirus, Machine Learning and Genetic Malware Detection	8
Initial Sample	8
Dropped Files	8
Unpacked PE Files	8
Domains	9
URLs	9
Domains and IPs	9
Contacted Domains	9
URLs from Memory and Binaries	10
World Map of Contacted IPs	13
Public IPs	13
General Information	14
Warnings	14
Simulations	14
Behavior and APIs	14
Joe Sandbox View / Context	14
IPs	14
Domains	15
ASNs	15
JA3 Fingerprints	15
Dropped Files	15
Created / dropped Files	15
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\WdFVsOe.exe.log	15
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\payment copy.exe.log	15
C:\Users\user\AppData\Roaming\WdFVsOe\WdFVsOe.exe	16
C:\Users\user\AppData\Roaming\WdFVsOe\WdFVsOe.exe:Zone.Identifier	16
Static File Info	16
General	16
File Icon	17
Static PE Info	17
General	17
Entrypoint Preview	17
Data Directories	19
Sections	19
Resources	19
Imports	19
Network Behavior	20
Network Port Distribution	20
TCP Packets	20
UDP Packets	22
DNS Queries	22
DNS Answers	22
SMTP Packets	22
Statistics	23
Behavior	23

System Behavior	23
Analysis Process: payment copy.exePID: 6064, Parent PID: 3452	23
General	23
File Activities	24
File Created	24
File Written	24
File Read	24
Analysis Process: payment copy.exePID: 1848, Parent PID: 6064	25
General	25
File Activities	25
File Created	25
File Written	26
File Read	26
Registry Activities	27
Key Value Created	27
Analysis Process: WdFVsOe.exePID: 5864, Parent PID: 3452	27
General	27
File Activities	27
File Created	27
File Written	28
File Read	28
Analysis Process: WdFVsOe.exePID: 5304, Parent PID: 5864	28
General	28
File Activities	29
File Created	29
File Read	29
Analysis Process: WdFVsOe.exePID: 4640, Parent PID: 3452	29
General	29
File Activities	30
File Created	30
File Read	30
Analysis Process: WdFVsOe.exePID: 612, Parent PID: 4640	30
General	30
Analysis Process: WdFVsOe.exePID: 2728, Parent PID: 4640	31
General	31
File Activities	31
File Created	31
File Read	31
Disassembly	32

Windows Analysis Report

payment copy.exe

Overview

General Information

Sample Name:	payment copy.exe
Analysis ID:	756033
MD5:	52fcd3f3cb7f0ea...
SHA1:	5a7304f89ce652..
SHA256:	eeabb0a04ea596.
Tags:	exe
Infos:	

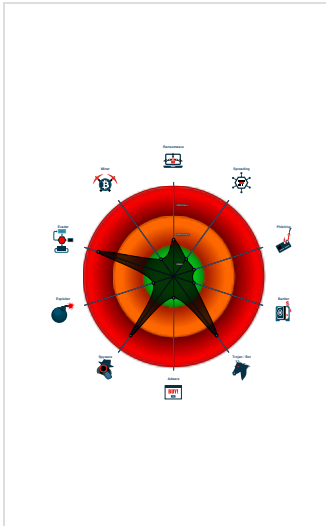
Detection

MALICIOUS SUSPICIOUS CLEAN UNKNOWN AgentTesla	
Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

Multi AV Scanner detection for subm...
Malicious sample detected (through...
Yara detected AgentTesla
Yara detected AntiVM3
Multi AV Scanner detection for drop...
Tries to steal Mail credentials (via fi...
Initial sample is a PE file and has a...
Tries to harvest and steal Putty / W...
Tries to harvest and steal ftp login c...
Tries to detect sandboxes and other...
Machine Learning detection for sam...
.NET source code contains very larg...

Classification



Process Tree

System is w10x64
payment copy.exe (PID: 6064 cmdline: C:\Users\user\Desktop\payment copy.exe MD5: 52FCD3F3CB7F0EAACC6CC393BA9313DA)
payment copy.exe (PID: 1848 cmdline: C:\Users\user\Desktop\payment copy.exe MD5: 52FCD3F3CB7F0EAACC6CC393BA9313DA)
WdFVsOe.exe (PID: 5864 cmdline: "C:\Users\user\AppData\Roaming\WdFVsOe\WdFVsOe.exe" MD5: 52FCD3F3CB7F0EAACC6CC393BA9313DA)
WdFVsOe.exe (PID: 5304 cmdline: C:\Users\user\AppData\Roaming\WdFVsOe\WdFVsOe.exe MD5: 52FCD3F3CB7F0EAACC6CC393BA9313DA)
WdFVsOe.exe (PID: 4640 cmdline: "C:\Users\user\AppData\Roaming\WdFVsOe\WdFVsOe.exe" MD5: 52FCD3F3CB7F0EAACC6CC393BA9313DA)
WdFVsOe.exe (PID: 612 cmdline: C:\Users\user\AppData\Roaming\WdFVsOe\WdFVsOe.exe MD5: 52FCD3F3CB7F0EAACC6CC393BA9313DA)
WdFVsOe.exe (PID: 2728 cmdline: C:\Users\user\AppData\Roaming\WdFVsOe\WdFVsOe.exe MD5: 52FCD3F3CB7F0EAACC6CC393BA9313DA)
cleanup

Malware Configuration

Threatname: Agenttesla

<pre>{ "Exfil Mode": "SMTP", "Host": "host39.registrar-servers.com", "Username": "Emenike@potashin.us", "Password": "}}cZs aj5Xr; c" }</pre>

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
0000000B.00000002.310942786.000000000325E000.0000004.00000800.00020000.00000000.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	

Source	Rule	Description	Author	Strings
0000000C.00000002.521910892.000000000323C000.0000004.00000800.00020000.00000000.sdm	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000C.00000002.521910892.000000000323C000.0000004.00000800.00020000.00000000.sdm	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000001.00000000.258978020.000000000402000.00000040.00000400.00020000.00000000.sdm	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000001.00000000.258978020.000000000402000.00000040.00000400.00020000.00000000.sdm	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 22 entries				

Unpacked PEs				
Source	Rule	Description	Author	Strings
0.2.payment copy.exe.474a140.7.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.payment copy.exe.474a140.7.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.payment copy.exe.474a140.7.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	0x32c0b:\$s10: logins 0x32685:\$s11: credential 0x2e8d5:\$g1: get_Clipboard 0x2e8e3:\$g2: get_Keyboard 0x2e8f0:\$g3: get_Password 0x2fca0:\$g4: get_CtrlKeyDown 0x2fcb0:\$g5: get_ShiftKeyDown 0x2fcc1:\$g6: get_AltKeyDown
0.2.payment copy.exe.474a140.7.unpack	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	0x300b6:\$a13: get_DnsResolver 0x2e7c3:\$a20: get_LastAccessed 0x30ae4:\$a27: set_InternalServerPort 0x30e19:\$a30: set_GuidMasterKey 0x2e8d5:\$a33: get_Clipboard 0x2e8e3:\$a34: get_Keyboard 0x2fcb0:\$a35: get_ShiftKeyDown 0x2fcc1:\$a36: get_AltKeyDown 0x2e8f0:\$a37: get_Password 0x2f40b:\$a38: get_PasswordHash 0x30518:\$a39: get_DefaultCredentials
1.0.payment copy.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 25 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection



Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

System Summary



Malicious sample detected (through community Yara rule)
Initial sample is a PE file and has a suspicious name
.NET source code contains very large array initializations

Hooking and other Techniques for Hiding and Protection



Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion



Yara detected AntiVM3
Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)
Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)
Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

Stealing of Sensitive Information



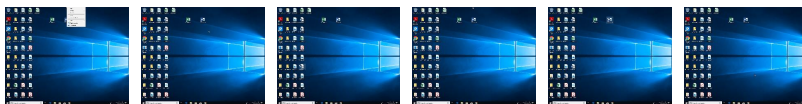
Yara detected AgentTesla
Tries to steal Mail credentials (via file / registry access)
Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)
Tries to harvest and steal ftp login credentials
Tries to harvest and steal browser information (history, passwords, etc)

Remote Access Functionality



Yara detected AgentTesla

Mitre Att&ck Matrix													
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	211 Windows Management Instrumentation	1 Registry Run Keys / Startup Folder	11 Process Injection	1 Disable or Modify Tools	2 OS Credential Dumping	114 System Information Discovery	Remote Services	11 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	2 Command and Scripting Interpreter	Boot or Logon Initialization Scripts	1 Registry Run Keys / Startup Folder	1 Deobfuscate/Decode Files or Information	1 Credentials in Registry	311 Security Software Discovery	Remote Desktop Protocol	2 Data from Local System	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	2 Obfuscated Files or Information	Security Account Manager	1 Process Discovery	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	3 Software Packing	NTDS	131 Virtualization/Sandbox Evasion	Distributed Component Object Model	Input Capture	Scheduled Transfer	11 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Masquerading	LSA Secrets	1 Application Window Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	131 Virtualization/Sandbox Evasion	Cached Domain Credentials	1 Remote System Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	11 Process Injection	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
payment copy.exe	30%	ReversingLabs	Win32.Trojan.Wore flint	
payment copy.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\WdFVsOe\WdFVsOe.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\WdFVsOe\WdFVsOe.exe	30%	ReversingLabs	Win32.Trojan.Wore flint	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.0.payment copy.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

 No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://crl.microsoft	0%	URL Reputation	safe	
http://crl.microsoft	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.comypo	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cnht	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cnn	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.typography.net	0%	URL Reputation	safe	
http://www.fontbureau.comB.TTF	0%	URL Reputation	safe	
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.monotype.95n	0%	Avira URL Cloud	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.carterandcone.comig	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	0%	URL Reputation	safe	
http://www.fontbureau.co	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.fontbureau.como	0%	URL Reputation	safe	
http://crl.micros	0%	URL Reputation	safe	
http://https://wINwvqrEjRpr.net8	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cn0	0%	Avira URL Cloud	safe	
http://ocsp.sectigo.com09	0%	Avira URL Cloud	safe	
http://vpDUpe.com	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cndf	0%	Avira URL Cloud	safe	
http://https://wINwvqrEjRpr.net	0%	Avira URL Cloud	safe	
http://www.fontbureau.comldwatR8	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cno.m	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
host39.registrar-servers.com	68.65.122.214	true	false		high

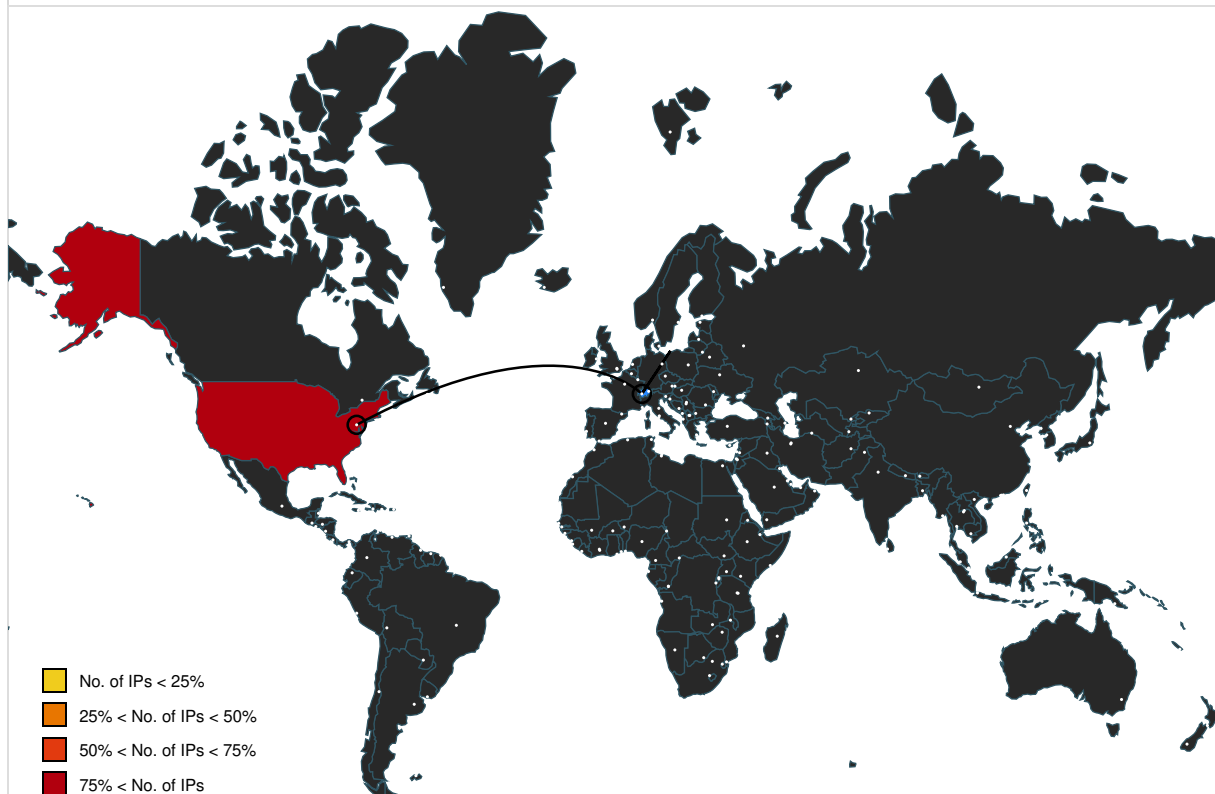
URLs from Memory and Binaries					
Name	Source	Malicious	Antivirus Detection	Reputation	
http://127.0.0.1:HTTP/1.1	payment copy.exe, 00000001.00000002.522170606.0000000003291000.00000004.00000800.00020000.00000000.sdmp, WdFVsOe.exe, 0000000C.00000002.521910892.000000000323C000.00000004.00000800.00020000.00000000.sdmp, WdFVsOe.exe, 0000000F.00000002.520858621.000000003361000.00000004.00000800.00020000.00000000.sdmp	false	Avira URL Cloud: safe	low	
http://www.fontbureau.com/designersG	payment copy.exe, 00000000.00000002.266294010.00000000074E2000.00000004.00000800.00020000.00000000.sdmp	false		high	
http://www.fontbureau.com/designers/?	payment copy.exe, 00000000.00000002.266294010.00000000074E2000.00000004.00000800.00020000.00000000.sdmp	false		high	
http://www.founder.com.cn/cn/bThe	payment copy.exe, 00000000.00000002.266294010.00000000074E2000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown	
http://www.fontbureau.com/designers8&	payment copy.exe, 00000000.00000003.251240828.00000000062E8000.00000004.00000800.00020000.00000000.sdmp, payment copy.exe, 00000000.00000003.250252956.00000000062E8000.00000004.00000800.00020000.00000000.sdmp	false		high	
http://crl.microsoft	WdFVsOe.exe, 0000000F.00000003.392037383.0000000006E4C000.00000004.00000800.00020000.00000000.sdmp	false	- URL Reputation: safe - URL Reputation: safe	unknown	
http://www.fontbureau.com/designers?	payment copy.exe, 00000000.00000002.266294010.00000000074E2000.00000004.00000800.00020000.00000000.sdmp	false		high	
http://vpDUpe.com	WdFVsOe.exe, 0000000F.00000002.520858621.000000003361000.00000004.00000800.00020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown	
http://www.monotype.95n	payment copy.exe, 00000000.00000003.250243768.00000000062DD000.00000004.00000800.00020000.00000000.sdmp, payment copy.exe, 00000000.00000003.250205326.00000000062DC000.00000004.00000800.00020000.00000000.sdmp	false	Avira URL Cloud: safe	low	
http://www.tiro.com	payment copy.exe, 00000000.00000002.266294010.00000000074E2000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown	
http://www.zhongyicts.com.cn0	payment copy.exe, 00000000.00000003.247858293.0000000006300000.00000004.00000800.00020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown	
http://www.fontbureau.com/designers	payment copy.exe, 00000000.00000002.266294010.00000000074E2000.00000004.00000800.00020000.00000000.sdmp	false		high	
http://www.goodfont.co.kr	payment copy.exe, 00000000.00000002.266294010.00000000074E2000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown	
http://www.carterandcone.com	payment copy.exe, 00000000.00000003.248035060.0000000006300000.00000004.00000800.00020000.00000000.sdmp, payment copy.exe, 00000000.00000003.247967738.0000000006300000.00000004.00000800.00020000.00000000.sdmp, payment copy.exe, 00000000.00000003.248057940.0000000006300000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown	
http://www.carterandcone.comypo	payment copy.exe, 00000000.00000003.248035060.0000000006300000.00000004.00000800.00020000.00000000.sdmp, payment copy.exe, 00000000.00000003.247967738.0000000006300000.00000004.00000800.00020000.00000000.sdmp, payment copy.exe, 00000000.00000003.248057940.0000000006300000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown	
http://www.sajatypeworks.com	payment copy.exe, 00000000.00000002.266294010.00000000074E2000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown	

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cnht	payment copy.exe, 00000000.00000003.247520874.0000000062FD000.00000004.00000800.00020000.00000000.sdmp, payment copy.exe, 00000000.00000003.247497084.0000000062FD000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	payment copy.exe, 00000000.00000002.266294010.0000000074E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	payment copy.exe, 00000000.00000002.266294010.0000000074E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cnn	payment copy.exe, 00000000.00000003.247520874.0000000062FD000.00000004.00000800.00020000.00000000.sdmp, payment copy.exe, 00000000.00000003.247497084.0000000062FD000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	payment copy.exe, 00000000.00000002.266294010.0000000074E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	payment copy.exe, 00000000.00000002.266294010.0000000074E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.net	payment copy.exe, 00000000.00000003.246833567.0000000062E0000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comB.TTF	payment copy.exe, 00000000.00000003.260213566.0000000062D0000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://DynDns.comDynDNSnamejdpaswordPsi/Psi	WdFVsOe.exe, 0000000F.00000002.520858621.000000003361000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://wlNwvqrEjRpr.net8	WdFVsOe.exe, 0000000C.00000002.532509205.00000000357A000.00000004.00000800.00020000.00000000.sdmp, WdFVsOe.exe, 0000000F.00000002.531668173.0000000036A7000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	payment copy.exe, 00000000.00000002.266294010.0000000074E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.ascendercorp.com/typedesigners.html	payment copy.exe, 00000000.00000003.249126135.0000000062E8000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.com	payment copy.exe, 00000000.00000002.266294010.0000000074E2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	payment copy.exe, 00000000.00000002.266294010.0000000074E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	payment copy.exe, 00000000.00000002.266294010.0000000074E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	payment copy.exe, 00000000.00000002.266294010.0000000074E2000.00000004.00000800.00020000.00000000.sdmp, payment copy.exe, 00000000.00000003.247858293.000000006300000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.com	payment copy.exe, 00000000.00000002.266294010.0000000074E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comig	payment copy.exe, 00000000.00000003.248035060.000000006300000.00000004.00000800.00020000.00000000.sdmp, payment copy.exe, 00000000.00000003.247967738.000000006300000.00000004.00000800.00020000.00000000.sdmp, payment copy.exe, 00000000.00000003.248057940.000000006300000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	payment copy.exe, 00000001.00000002.533327699.00000000360E000.00000004.00000800.00020000.00000000.sdmp, WdFVsOe.exe, 0000000C.00000002.533250375.0000000035B8000.00000004.00000800.00020000.00000000.sdmp, WdFVsOe.exe, 0000000F.00000002.531668173.0000000036A7000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	payment copy.exe, 00000000.00000002.2662 94010.00000000074E2000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://www.fontbureau.com	payment copy.exe, 00000000.00000002.2662 94010.00000000074E2000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersDF-	payment copy.exe, 00000000.00000003.2502 52956.00000000062E8000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://https://sectigo.com/CPS0	payment copy.exe, 00000001.00000002.5333 27699.000000000360E000.00000004.00000800 .00020000.00000000.sdmp, WdFVsOe.exe, 00 00000C.00000002.533250375.00000000035B80 00.00000004.00000800.00020000.00000000.sdmp, WdFVsOe.exe, 0000000F.00000002.531668173.0000 0000036A7000.00000004.00000800.00020000. 00000000.sdmp	false	- URL Reputation: safe - URL Reputation: safe	unknown
http://ocsp.sectigo.com09	payment copy.exe, 00000001.00000002.5333 27699.000000000360E000.00000004.00000800 .00020000.00000000.sdmp, WdFVsOe.exe, 00 00000C.00000002.533250375.00000000035B80 00.00000004.00000800.00020000.00000000.sdmp, WdFVsOe.exe, 0000000F.00000002.531668173.0000 0000036A7000.00000004.00000800.00020000. 00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers~	payment copy.exe, 00000000.00000003.2512 40828.00000000062E8000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://host39.registrar-servers.com	payment copy.exe, 00000001.00000002.5333 27699.000000000360E000.00000004.00000800 .00020000.00000000.sdmp, WdFVsOe.exe, 00 00000C.00000002.533250375.00000000035B80 00.00000004.00000800.00020000.00000000.sdmp, WdFVsOe.exe, 0000000F.00000002.531668173.0000 0000036A7000.00000004.00000800.00020000. 00000000.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	payment copy.exe, 00000001.00000002.5221 70606.0000000003291000.00000004.00000800 .00020000.00000000.sdmp, WdFVsOe.exe, 00 00000C.00000002.521910892.00000000032C0 00.00000004.00000800.00020000.00000000.sdmp, WdFVsOe.exe, 0000000F.00000002.520858621.0000 000003361000.00000004.00000800.00020000. 00000000.sdmp	false	URL Reputation: safe	unknown
http://www.fontbureau.co	payment copy.exe, 00000000.00000003.2509 90543.000000000631E000.00000004.00000800 .00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.founder.com.cn/cndf	payment copy.exe, 00000000.00000003.2475 20874.00000000062FD000.00000004.00000800 .00020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	payment copy.exe, 00000000.00000002.2662 94010.00000000074E2000.00000004.00000800 .00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.founder.com.cn/cn/	payment copy.exe, 00000000.00000003.2476 75536.0000000006300000.00000004.00000800 .00020000.00000000.sdmp, payment copy.exe, 00000000.00000003.247640305.00000000 62FE000.00000004.00000800.00020000.00000 000.sdmp	false	URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	payment copy.exe, 00000000.00000002.2662 94010.00000000074E2000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn	payment copy.exe, 00000000.00000002.2662 94010.00000000074E2000.00000004.00000800 .00020000.00000000.sdmp, payment copy.exe, 00000000.00000003.247640305.00000000 62FE000.00000004.00000800.00020000.00000 000.sdmp	false	URL Reputation: safe	unknown
http://https://wlNvwqrEjRpr.net	WdFVsOe.exe, 0000000F.00000002.531668173 .00000000036A7000.00000004.00000800.0002 0000.00000000.sdmp	false	Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/frere-jones.html	payment copy.exe, 00000000.00000003.250921715.000000000631E000.00000004.00000800.00020000.00000000.sdmp, payment copy.exe, 00000000.00000003.250791703.000000000631E000.00000004.00000800.00020000.00000000000.sdmp, payment copy.exe, 00000000.00000003.250690710.000000000631E000.00000004.00000800.00020000.00000000000.sdmp, payment copy.exe, 00000000.00000003.250751911.000000000631E000.00000004.00000800.00020000.00000000000.sdmp, payment copy.exe, 00000000.00000003.250850742.000000000631E000.00000004.00000800.00020000.00000000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/	payment copy.exe, 00000000.00000002.266294010.00000000074E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com	payment copy.exe, 00000000.00000003.260213566.00000000062D0000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	payment copy.exe, 00000000.00000002.266294010.00000000074E2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.zhongyicts.com.cno.m	payment copy.exe, 00000000.00000003.247858293.0000000006300000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comldwatR8	payment copy.exe, 00000000.00000003.260213566.00000000062D0000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.micros	payment copy.exe, 00000001.00000002.541820691.000000000674E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
68.65.122.214	host39.registrar-servers.com	United States		22612	NAMECHEAP-NETUS	false

General Information	
Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	756033
Start date and time:	2022-11-29 14:54:07 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 36s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	payment copy.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	18
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@11/4@3/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 95% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings
• Exclude process from analysis (whitelisted): MpCmdRun.exe, SgrmBroker.exe, conhost.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded domains from analysis (whitelisted): fs.microsoft.com • Not all processes where analyzed, report is missing behavior information • Report creation exceeded maximum time and may have missing disassembly code information. • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations		
Behavior and APIs		
Time	Type	Description
14:55:04	API Interceptor	663x Sleep call for process: payment copy.exe modified
14:55:14	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run WdFVsOe C:\Users\user\AppData\Roaming\WdFVsOe\WdFVsOe.exe
14:55:22	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run WdFVsOe C:\Users\user\AppData\Roaming\WdFVsOe\WdFVsOe.exe
14:55:25	API Interceptor	855x Sleep call for process: WdFVsOe.exe modified

Joe Sandbox View / Context
IPs

 No context

Domains
 No context

ASNs
 No context

JA3 Fingerprints
 No context

Dropped Files
 No context

Created / dropped Files	
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\WdFVs0e.exe.log	
Process:	C:\Users\user\AppData\Roaming\WdFVs0e\WdFVs0e.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178FF6
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\1f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a", "C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\payment copy.exe.log 	
Process:	C:\Users\user\Desktop\payment copy.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178FF6
Malicious:	true
Reputation:	high, very likely benign file

Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\1f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\1b219d4630d26b88041b59c21
----------	---

C:\Users\user\AppData\Roaming\WdFVs0e\WdFVs0e.exe  	
Process:	C:\Users\user\Desktop\payment copy.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	963072
Entropy (8bit):	7.666020966282773
Encrypted:	false
SSDEEP:	12288:yEhqU+PoxVZ861s4cEOSJi0yIYqQo/tdYV71JSYVBgrVDdzoa1cfN:LuoxL1MEPzyIBPY/JSMBgBDdEPf
MD5:	52FCD3F3CB7F0EAACC6CC393BA9313DA
SHA1:	5A7304F89CE6525E0449FFDF0022F5114D181680
SHA-256:	EEABB0A04EA59624D05185AFBBF4A1C8E5DB554C0C325871C4C0AC5DE34C5547
SHA-512:	7CE8744C23B517043B25F173733888385BE9FDDAA67B597C3EC522D24D422ED1FEE9A44CFA51C7C6C3812FBC2FD791FE57A822E3C0A462670448FB0EE507C54FC
Malicious:	true
Antivirus:	- Antivirus: Joe Sandbox ML, Detection: 100% - Antivirus: ReversingLabs, Detection: 30%
Reputation:	low
Preview:	MZ.....@.....!..!This program cannot be run in DOS mode....\$.....PE..L....c.....0.....z.....@..... ..@.....\.....O.....H.....text.....\......rsrc.....@.....@.reloc.....@..B.....H.....<.....l..8u..S.....^.).....(.....*.0.....s.....o.....(.....*.0.....s.....o.....(.....*.0.....s.....o.....(..... *.0.....s.....o.....(.....*.0..+.....{.....+.....{.....0.....(.....*.0..f.....(.....s.....s.....).....s.....).....(.....{.....0.....{.....0.....{.....f...p"..@A..s! ..o".....{.....(#...o\$.....{..... ..

C:\Users\user\AppData\Roaming\WdFVs0e\WdFVs0e.exe:Zone.Identifier 	
Process:	C:\Users\user\Desktop\payment copy.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD6E
Malicious:	true
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info	
General	
File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.666020966282773
TrID:	- Win32 Executable (generic) Net Framework (10011505/4) 49.80% - Win32 Executable (generic) a (10002005/4) 49.75% - Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% - Windows Screen Saver (13104/52) 0.07% - Generic Win/DOS Executable (2004/3) 0.01%
File name:	payment copy.exe
File size:	963072
MD5:	52fcd3f3cb7f0eaacc6cc393ba9313da
SHA1:	5a7304f89ce6525e0449ffdf0022f5114d181680

SHA256:	eeabb0a04ea59624d05185afbfb4a1c8e5db554c0c325871c4c0ac5de34c5547
SHA512:	7ce8744c23b517043b25f173733888385be9fdaa67b597c3ec522d24d422ed1fee9a44cfa51c7c6c3812fbc2fd791fe57a822e3c0a462670448fb0ee507c54ec
SSDEEP:	12288:yEhQ+PoxVZ861s4cEOSJJi0ylxYeQo/tdYV71JSYVBgrVDdzoa1cfn:LuoxL1MEPzylBPY/JSMBgBDdEPf
TLSH:	3F25E08033A6BF71F5696BF37521800827763C6EA5E0D6285DCDB0DE2A76B5049F0B27
File Content Preview:	MZ.....!..L!This program cannot be run in DOS mode....\$......PE..L.....c.....0.....z.....@..@.....

File Icon



Icon Hash:	00828e8e8686b000
------------	------------------

Static PE Info

General

Entrypoint:	0x4ec97a
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x6385B1CA [Tue Nov 29 07:16:26 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction

```
jmp dword ptr [00402000h]
```

```
add byte ptr [eax], al
```

```
add byte ptr [eax], al
```

```
add byte ptr [eax], al
```

```
add byte ptr [eax], al
```

```
add byte ptr [eax], al
```

```
add byte ptr [eax], al
```

```
add byte ptr [eax], al
```

```
add byte ptr [eax], al
```

```
add byte ptr [eax], al
```

```
add byte ptr [eax], al
```

```
add byte ptr [eax], al
```

```
add byte ptr [eax], al
```

```
add byte ptr [eax], al
```

```
add byte ptr [eax], al
```

```
add byte ptr [eax], al
```

```
add byte ptr [eax], al
```

```
add byte ptr [eax], al
```

```
add byte ptr [eax], al
```

```
add byte ptr [eax], al
```

```
add byte ptr [eax], al
```

```
add byte ptr [eax], al
```

```
add byte ptr [eax], al
```

```
add byte ptr [eax], al
```


Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories			
Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xec928	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xee000	0x388	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xf0000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

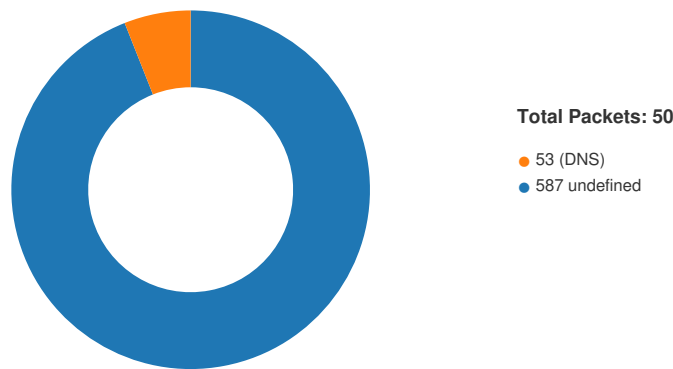
Sections								
Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xea980	0xeaa00	False	0.8303174530500799	data	7.672485147748669	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xee000	0x388	0x400	False	0.37109375	data	2.8467797153196712	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.reloc	0xf0000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources						
Name	RVA	Size	Type	Language	Country	
RT_VERSION	0xee058	0x32c	data			

Imports	
DLL	Import
mscorlib.dll	_CorExeMain

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 14:55:25.424974918 CET	49699	587	192.168.2.3	68.65.122.214
Nov 29, 2022 14:55:25.592058897 CET	587	49699	68.65.122.214	192.168.2.3
Nov 29, 2022 14:55:25.592273951 CET	49699	587	192.168.2.3	68.65.122.214
Nov 29, 2022 14:55:25.895911932 CET	587	49699	68.65.122.214	192.168.2.3
Nov 29, 2022 14:55:25.905392885 CET	49699	587	192.168.2.3	68.65.122.214
Nov 29, 2022 14:55:26.075438023 CET	587	49699	68.65.122.214	192.168.2.3
Nov 29, 2022 14:55:26.075676918 CET	49699	587	192.168.2.3	68.65.122.214
Nov 29, 2022 14:55:26.248148918 CET	587	49699	68.65.122.214	192.168.2.3
Nov 29, 2022 14:55:26.295599937 CET	49699	587	192.168.2.3	68.65.122.214
Nov 29, 2022 14:55:26.479507923 CET	587	49699	68.65.122.214	192.168.2.3
Nov 29, 2022 14:55:26.479547024 CET	587	49699	68.65.122.214	192.168.2.3
Nov 29, 2022 14:55:26.479569912 CET	587	49699	68.65.122.214	192.168.2.3
Nov 29, 2022 14:55:26.479587078 CET	587	49699	68.65.122.214	192.168.2.3
Nov 29, 2022 14:55:26.479638100 CET	49699	587	192.168.2.3	68.65.122.214
Nov 29, 2022 14:55:26.479693890 CET	49699	587	192.168.2.3	68.65.122.214
Nov 29, 2022 14:55:26.481981993 CET	587	49699	68.65.122.214	192.168.2.3
Nov 29, 2022 14:55:26.535485983 CET	49699	587	192.168.2.3	68.65.122.214
Nov 29, 2022 14:55:26.703422070 CET	587	49699	68.65.122.214	192.168.2.3
Nov 29, 2022 14:55:26.763364077 CET	49699	587	192.168.2.3	68.65.122.214
Nov 29, 2022 14:55:26.930888891 CET	587	49699	68.65.122.214	192.168.2.3
Nov 29, 2022 14:55:26.933207035 CET	49699	587	192.168.2.3	68.65.122.214
Nov 29, 2022 14:55:27.102840900 CET	587	49699	68.65.122.214	192.168.2.3
Nov 29, 2022 14:55:27.103601933 CET	49699	587	192.168.2.3	68.65.122.214
Nov 29, 2022 14:55:27.310229063 CET	587	49699	68.65.122.214	192.168.2.3
Nov 29, 2022 14:55:27.324902058 CET	587	49699	68.65.122.214	192.168.2.3
Nov 29, 2022 14:55:27.326145887 CET	49699	587	192.168.2.3	68.65.122.214
Nov 29, 2022 14:55:27.492806911 CET	587	49699	68.65.122.214	192.168.2.3
Nov 29, 2022 14:55:27.492857933 CET	587	49699	68.65.122.214	192.168.2.3
Nov 29, 2022 14:55:27.493326902 CET	49699	587	192.168.2.3	68.65.122.214
Nov 29, 2022 14:55:27.666775942 CET	587	49699	68.65.122.214	192.168.2.3
Nov 29, 2022 14:55:27.667530060 CET	49699	587	192.168.2.3	68.65.122.214
Nov 29, 2022 14:55:27.835021019 CET	587	49699	68.65.122.214	192.168.2.3
Nov 29, 2022 14:55:27.837627888 CET	49699	587	192.168.2.3	68.65.122.214
Nov 29, 2022 14:55:27.837723017 CET	49699	587	192.168.2.3	68.65.122.214
Nov 29, 2022 14:55:27.838565111 CET	49699	587	192.168.2.3	68.65.122.214
Nov 29, 2022 14:55:27.838650942 CET	49699	587	192.168.2.3	68.65.122.214
Nov 29, 2022 14:55:28.008394957 CET	587	49699	68.65.122.214	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 14:55:28.008449078 CET	587	49699	68.65.122.214	192.168.2.3
Nov 29, 2022 14:55:28.008755922 CET	587	49699	68.65.122.214	192.168.2.3
Nov 29, 2022 14:55:28.014305115 CET	587	49699	68.65.122.214	192.168.2.3
Nov 29, 2022 14:55:28.155173063 CET	49699	587	192.168.2.3	68.65.122.214
Nov 29, 2022 14:55:56.683109999 CET	49700	587	192.168.2.3	68.65.122.214
Nov 29, 2022 14:55:56.851603031 CET	587	49700	68.65.122.214	192.168.2.3
Nov 29, 2022 14:55:56.852837086 CET	49700	587	192.168.2.3	68.65.122.214
Nov 29, 2022 14:55:57.171015978 CET	587	49700	68.65.122.214	192.168.2.3
Nov 29, 2022 14:55:57.173106909 CET	49700	587	192.168.2.3	68.65.122.214
Nov 29, 2022 14:55:57.341361046 CET	587	49700	68.65.122.214	192.168.2.3
Nov 29, 2022 14:55:57.341626883 CET	49700	587	192.168.2.3	68.65.122.214
Nov 29, 2022 14:55:57.512027979 CET	587	49700	68.65.122.214	192.168.2.3
Nov 29, 2022 14:55:57.544939995 CET	49700	587	192.168.2.3	68.65.122.214
Nov 29, 2022 14:55:57.730178118 CET	587	49700	68.65.122.214	192.168.2.3
Nov 29, 2022 14:55:57.730206966 CET	587	49700	68.65.122.214	192.168.2.3
Nov 29, 2022 14:55:57.730222940 CET	587	49700	68.65.122.214	192.168.2.3
Nov 29, 2022 14:55:57.730238914 CET	587	49700	68.65.122.214	192.168.2.3
Nov 29, 2022 14:55:57.730304956 CET	49700	587	192.168.2.3	68.65.122.214
Nov 29, 2022 14:55:57.732626915 CET	587	49700	68.65.122.214	192.168.2.3
Nov 29, 2022 14:55:57.747056007 CET	49700	587	192.168.2.3	68.65.122.214
Nov 29, 2022 14:55:57.915951967 CET	587	49700	68.65.122.214	192.168.2.3
Nov 29, 2022 14:55:57.997579098 CET	49700	587	192.168.2.3	68.65.122.214
Nov 29, 2022 14:55:58.166379929 CET	587	49700	68.65.122.214	192.168.2.3
Nov 29, 2022 14:55:58.166922092 CET	49700	587	192.168.2.3	68.65.122.214
Nov 29, 2022 14:55:58.335804939 CET	587	49700	68.65.122.214	192.168.2.3
Nov 29, 2022 14:55:58.336447954 CET	49700	587	192.168.2.3	68.65.122.214
Nov 29, 2022 14:55:58.521548033 CET	587	49700	68.65.122.214	192.168.2.3
Nov 29, 2022 14:55:58.522005081 CET	49700	587	192.168.2.3	68.65.122.214
Nov 29, 2022 14:55:58.691117048 CET	587	49700	68.65.122.214	192.168.2.3
Nov 29, 2022 14:55:58.691618919 CET	49700	587	192.168.2.3	68.65.122.214
Nov 29, 2022 14:55:58.867047071 CET	587	49700	68.65.122.214	192.168.2.3
Nov 29, 2022 14:55:58.867399931 CET	49700	587	192.168.2.3	68.65.122.214
Nov 29, 2022 14:55:59.037381887 CET	587	49700	68.65.122.214	192.168.2.3
Nov 29, 2022 14:55:59.038328886 CET	49700	587	192.168.2.3	68.65.122.214
Nov 29, 2022 14:55:59.038417101 CET	49700	587	192.168.2.3	68.65.122.214
Nov 29, 2022 14:55:59.038485050 CET	49700	587	192.168.2.3	68.65.122.214
Nov 29, 2022 14:55:59.038551092 CET	49700	587	192.168.2.3	68.65.122.214
Nov 29, 2022 14:55:59.217993021 CET	587	49700	68.65.122.214	192.168.2.3
Nov 29, 2022 14:55:59.218055964 CET	587	49700	68.65.122.214	192.168.2.3
Nov 29, 2022 14:55:59.227782011 CET	587	49700	68.65.122.214	192.168.2.3
Nov 29, 2022 14:55:59.227830887 CET	587	49700	68.65.122.214	192.168.2.3
Nov 29, 2022 14:55:59.273787022 CET	49700	587	192.168.2.3	68.65.122.214
Nov 29, 2022 14:56:06.216950893 CET	49701	587	192.168.2.3	68.65.122.214
Nov 29, 2022 14:56:06.384685993 CET	587	49701	68.65.122.214	192.168.2.3
Nov 29, 2022 14:56:06.384807110 CET	49701	587	192.168.2.3	68.65.122.214
Nov 29, 2022 14:56:06.619520903 CET	587	49701	68.65.122.214	192.168.2.3
Nov 29, 2022 14:56:06.620049000 CET	49701	587	192.168.2.3	68.65.122.214
Nov 29, 2022 14:56:06.790031910 CET	587	49701	68.65.122.214	192.168.2.3
Nov 29, 2022 14:56:06.793853045 CET	49701	587	192.168.2.3	68.65.122.214
Nov 29, 2022 14:56:06.964744091 CET	587	49701	68.65.122.214	192.168.2.3
Nov 29, 2022 14:56:06.980041027 CET	49701	587	192.168.2.3	68.65.122.214
Nov 29, 2022 14:56:07.162103891 CET	587	49701	68.65.122.214	192.168.2.3
Nov 29, 2022 14:56:07.162137032 CET	587	49701	68.65.122.214	192.168.2.3
Nov 29, 2022 14:56:07.162158966 CET	587	49701	68.65.122.214	192.168.2.3
Nov 29, 2022 14:56:07.162178993 CET	587	49701	68.65.122.214	192.168.2.3
Nov 29, 2022 14:56:07.162257910 CET	49701	587	192.168.2.3	68.65.122.214
Nov 29, 2022 14:56:07.165424109 CET	587	49701	68.65.122.214	192.168.2.3
Nov 29, 2022 14:56:07.167860031 CET	49701	587	192.168.2.3	68.65.122.214
Nov 29, 2022 14:56:07.336713076 CET	587	49701	68.65.122.214	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 14:56:07.392863035 CET	49701	587	192.168.2.3	68.65.122.214
Nov 29, 2022 14:56:07.420589924 CET	49701	587	192.168.2.3	68.65.122.214
Nov 29, 2022 14:56:07.599742889 CET	587	49701	68.65.122.214	192.168.2.3
Nov 29, 2022 14:56:07.603785038 CET	49701	587	192.168.2.3	68.65.122.214

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 14:55:25.373497963 CET	49977	53	192.168.2.3	8.8.8.8
Nov 29, 2022 14:55:25.394471884 CET	53	49977	8.8.8.8	192.168.2.3
Nov 29, 2022 14:55:56.601288080 CET	57840	53	192.168.2.3	8.8.8.8
Nov 29, 2022 14:55:56.621599913 CET	53	57840	8.8.8.8	192.168.2.3
Nov 29, 2022 14:56:06.164307117 CET	57990	53	192.168.2.3	8.8.8.8
Nov 29, 2022 14:56:06.181865931 CET	53	57990	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 29, 2022 14:55:25.373497963 CET	192.168.2.3	8.8.8.8	0x8bf7	Standard query (0)	host39.registrar-servers.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 14:55:56.601288080 CET	192.168.2.3	8.8.8.8	0x1ade	Standard query (0)	host39.registrar-servers.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 14:56:06.164307117 CET	192.168.2.3	8.8.8.8	0xea32	Standard query (0)	host39.registrar-servers.com	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 29, 2022 14:55:25.394471884 CET	8.8.8.8	192.168.2.3	0x8bf7	No error (0)	host39.registrar-servers.com		68.65.122.214	A (IP address)	IN (0x0001)	false
Nov 29, 2022 14:55:56.621599913 CET	8.8.8.8	192.168.2.3	0x1ade	No error (0)	host39.registrar-servers.com		68.65.122.214	A (IP address)	IN (0x0001)	false
Nov 29, 2022 14:56:06.181865931 CET	8.8.8.8	192.168.2.3	0xea32	No error (0)	host39.registrar-servers.com		68.65.122.214	A (IP address)	IN (0x0001)	false

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Nov 29, 2022 14:55:25.895911932 CET	587	49699	68.65.122.214	192.168.2.3	220-host39.registrar-servers.com ESMTP Exim 4.95 #2 Tue, 29 Nov 2022 08:55:25 -0500 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Nov 29, 2022 14:55:25.905392885 CET	49699	587	192.168.2.3	68.65.122.214	EHLO 332260
Nov 29, 2022 14:55:26.075438023 CET	587	49699	68.65.122.214	192.168.2.3	250-host39.registrar-servers.com Hello 332260 [102.129.143.49] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Nov 29, 2022 14:55:26.075676918 CET	49699	587	192.168.2.3	68.65.122.214	STARTTLS
Nov 29, 2022 14:55:26.248148918 CET	587	49699	68.65.122.214	192.168.2.3	220 TLS go ahead
Nov 29, 2022 14:55:57.171015978 CET	587	49700	68.65.122.214	192.168.2.3	220-host39.registrar-servers.com ESMTP Exim 4.95 #2 Tue, 29 Nov 2022 08:55:57 -0500 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Nov 29, 2022 14:55:57.173106909 CET	49700	587	192.168.2.3	68.65.122.214	EHLO 332260

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Nov 29, 2022 14:55:57.341361046 CET	587	49700	68.65.122.214	192.168.2.3	250-host39.registrar-servers.com Hello 332260 [102.129.143.49] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Nov 29, 2022 14:55:57.341626883 CET	49700	587	192.168.2.3	68.65.122.214	STARTTLS
Nov 29, 2022 14:55:57.512027979 CET	587	49700	68.65.122.214	192.168.2.3	220 TLS go ahead
Nov 29, 2022 14:56:06.619520903 CET	587	49701	68.65.122.214	192.168.2.3	220-host39.registrar-servers.com ESMTP Exim 4.95 #2 Tue, 29 Nov 2022 08:56:06 -0500 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Nov 29, 2022 14:56:06.620049000 CET	49701	587	192.168.2.3	68.65.122.214	EHLO 332260
Nov 29, 2022 14:56:06.790031910 CET	587	49701	68.65.122.214	192.168.2.3	250-host39.registrar-servers.com Hello 332260 [102.129.143.49] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Nov 29, 2022 14:56:06.793853045 CET	49701	587	192.168.2.3	68.65.122.214	STARTTLS
Nov 29, 2022 14:56:06.964744091 CET	587	49701	68.65.122.214	192.168.2.3	220 TLS go ahead

Statistics

Behavior

- payment copy.exe
- payment copy.exe
- WdFVsOe.exe
- WdFVsOe.exe
- WdFVsOe.exe
- WdFVsOe.exe
- WdFVsOe.exe

Click to jump to process

System Behavior

Analysis Process: payment copy.exe PID: 6064, Parent PID: 3452

General

Target ID:	0
Start time:	14:54:58
Start date:	29/11/2022
Path:	C:\Users\user\Desktop\payment copy.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\payment copy.exe
Imagebase:	0xf60000
File size:	963072 bytes

MD5 hash:	52FCD3F3CB7F0EAACC6CC393BA9313DA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.261250021.00000000033C1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.262257256.00000000036CE000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.263520436.000000000462B000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.263520436.000000000462B000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000000.00000002.263520436.000000000462B000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities								
File Created								
File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol	
C:\Users\user	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	6D1BCF06	unknown	
C:\Users\user\AppData\Roaming	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	6D1BCF06	unknown	
C:\Users\user\AppData\Local\Microsof\CLR_v4.0.32\UsageLogs\payment copy.exe.log	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	6D4CC78D	CreateFileW	

File Written									
File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol	
C:\Users\user\AppData\Local\Microsof\CLR_v4.0.32\UsageLogs\payment copy.exe.log	0	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089", "C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6D4CC907	WriteFile	

File Read							
File Path	Offset	Length	Completion	Count	Source Address	Symbol	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D195705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D195705	unknown	
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib.a152fe02a317a77ae36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D0F03DE	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D19CA54	ReadFile	

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbcb72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D0F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D0F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D0F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D195705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D195705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C001B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C001B4F	ReadFile

Analysis Process: payment copy.exe PID: 1848, Parent PID: 6064	
General	
Target ID:	1
Start time:	14:55:05
Start date:	29/11/2022
Path:	C:\Users\user\Desktop\payment copy.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\payment copy.exe
Imagebase:	0xda0000
File size:	963072 bytes
MD5 hash:	52FCD3F3CB7F0EAACC6CC393BA9313DA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	- Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000000.258978020.000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000000.258978020.000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security - Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000001.00000000.258978020.000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown - Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.522170606.0000000003291000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000002.522170606.0000000003291000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities							
File Created							
File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	6D1BCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	6D1BCF06	unknown
C:\Users\user\AppData\Roaming\WdFVsOe	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	6C00BEFF	CreateDirectoryW

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6C001B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002812f1102-a14c-4a8d-9bed-0b62191d8809	unknown	4096	success or wait	1	6C001B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6C001B4F	ReadFile
C:\Program Files (x86)\j\Downloader\config\database.script	unknown	4096	success or wait	1	6C001B4F	ReadFile
C:\Program Files (x86)\j\Downloader\config\database.script	unknown	4096	end of file	1	6C001B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default>Login Data	unknown	49152	success or wait	1	6C001B4F	ReadFile

Registry Activities							
Key Value Created							
Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	WdFVsOe	unicode	C:\Users\user\AppData\Roaming\WdFVsOe\WdFVsOe.exe	success or wait	1	6C00646A	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run	WdFVsOe	binary	02 00 00 00 00 00 00 00 00 00 00	success or wait	1	6C00DE2E	RegSetValueExW

Analysis Process: WdFVsOe.exe PID: 5864, Parent PID: 3452	
General	
Target ID:	11
Start time:	14:55:22
Start date:	29/11/2022
Path:	C:\Users\user\AppData\Roaming\WdFVsOe\WdFVsOe.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\WdFVsOe\WdFVsOe.exe"
Imagebase:	0xaf0000
File size:	963072 bytes
MD5 hash:	52FCD3F3CB7F0EAACC6CC393BA9313DA
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	- Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 0000000B.00000002.310942786.000000000325E000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 0000000B.00000002.307766391.0000000002F51000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	- Detection: 100%, Joe Sandbox ML - Detection: 30%, ReversingLabs
Reputation:	low

File Activities							
File Created							
File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	6D1BCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	6D1BCF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\WdFVsOe.exe.log	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	6D4CC78D	CreateFileW

File Written									
File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol	
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0.32\UsageLogs\WdFVsOe.exe.log	0	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NativeImages_v4.0.3",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089", "C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6D4CC907	WriteFile	

File Read							
File Path	Offset	Length	Completion	Count	Source Address	Symbol	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D195705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D195705	unknown	
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib.a152fe02a317a77ae36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D0F03DE	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D19CA54	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbcb72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0F03DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D0F03DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D0F03DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D0F03DE	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D195705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D195705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C001B4F	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C001B4F	ReadFile	

Analysis Process: WdFVsOe.exe PID: 5304, Parent PID: 5864	
General	
Target ID:	12
Start time:	14:55:27
Start date:	29/11/2022
Path:	C:\Users\user\AppData\Roaming\WdFVsOe\WdFVsOe.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\WdFVsOe\WdFVsOe.exe
Imagebase:	0xcd0000
File size:	963072 bytes
MD5 hash:	52FCD3F3CB7F0EAACC6CC393BA9313DA
Has elevated privileges:	false
Has administrator privileges:	false

Programmed in:	.Net C# or VB.NET
Yara matches:	- Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000C.00000002.521910892.000000000323C000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000C.00000002.521910892.000000000323C000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities								
File Created								
File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol	
C:\Users\user	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	6D1BCF06	unknown	
C:\Users\user\AppData\Roaming	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	6D1BCF06	unknown	
C:\Users\user\AppData\Local\Temp\tmpD430.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	6C007038	GetTempFile NameW	

File Read							
File Path	Offset	Length	Completion	Count	Source Address	Symbol	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D195705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D195705	unknown	
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib.a152fe02a317a77ae36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D0F03DE	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D19CA54	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbcb72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0F03DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D0F03DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D0F03DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D0F03DE	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D195705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D195705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C001B4F	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C001B4F	ReadFile	
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6C001B4F	ReadFile	
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002812f1102-a14c-4a8d-9bed-0b62191d8809	unknown	4096	success or wait	1	6C001B4F	ReadFile	
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6C001B4F	ReadFile	
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C001B4F	ReadFile	
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C001B4F	ReadFile	
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default>Login Data	unknown	49152	success or wait	1	6C001B4F	ReadFile	

Analysis Process: WdFVsOe.exe PID: 4640, Parent PID: 3452	
General	
Target ID:	13
Start time:	14:55:30
Start date:	29/11/2022
Path:	C:\Users\user\AppData\Roaming\WdFVsOe\WdFVsOe.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\WdFVsOe\WdFVsOe.exe"
Imagebase:	0x7c0000

File size:	963072 bytes
MD5 hash:	52FCD3F3CB7F0EAACC6CC393BA9313DA
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities								
File Created								
File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol	
C:\Users\user	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	6D1BCF06	unknown	
C:\Users\user\AppData\Roaming	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	6D1BCF06	unknown	

File Read							
File Path	Offset	Length	Completion	Count	Source Address	Symbol	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D195705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D195705	unknown	
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib.a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D0F03DE	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D19CA54	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0F03DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D0F03DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D0F03DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D0F03DE	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D195705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D195705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C001B4F	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C001B4F	ReadFile	

Analysis Process: WdFVsOe.exe PID: 612, Parent PID: 4640	
General	
Target ID:	14
Start time:	14:55:39
Start date:	29/11/2022
Path:	C:\Users\user\AppData\Roaming\WdFVsOe\WdFVsOe.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Roaming\WdFVsOe\WdFVsOe.exe
Imagebase:	0x380000
File size:	963072 bytes
MD5 hash:	52FCD3F3CB7F0EAACC6CC393BA9313DA
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: WdFVsOe.exe PID: 2728, Parent PID: 4640

General

Target ID:	15
Start time:	14:55:40
Start date:	29/11/2022
Path:	C:\Users\user\AppData\Roaming\WdFVsOe\WdFVsOe.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\WdFVsOe\WdFVsOe.exe
Imagebase:	0xdc0000
File size:	963072 bytes
MD5 hash:	52FCD3F3CB7F0EAACC6CC393BA9313DA
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	- Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000F.00000002.520858621.0000000003361000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000F.00000002.520858621.0000000003361000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	6D1BCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	6D1BCF06	unknown
C:\Users\user\AppData\Local\Temp\tmp831.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	6C007038	GetTempFile NameW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D195705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D195705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib.a152fe02a317a77ae36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D0F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D19CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbcb72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D0F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D0F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D0F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D195705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D195705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C001B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C001B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6C001B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\812f1102-a14c-4a8d-9bed-0b62191d8809	unknown	4096	success or wait	1	6C001B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6C001B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C001B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\j\Downloader\config\database.script	unknown	4096	end of file	1	6C001B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default>Login Data	unknown	49152	success or wait	1	6C001B4F	ReadFile

Disassembly

 No disassembly